

EXHIBIT I



Privacy Impact Assessment for
Electronic Official Personnel Folder
System (eOPF)

April 9, 2025

Contact Point

Nii-Kwashie Aryeetey
Director, eOPF Program
Human Resources Solutions Information Technology
Program Management Office (HRSITPMO)

Reviewing Official

Becky Ronayne
Acting Senior Agency Official for Privacy



Abstract

The electronic Official Personnel Folder system (eOPF) maintains the official digital imaged versions of the Official Personnel Folders (OPF) for Federal employees and contains various virtual work folders used by human resource offices. It also maintains records for non-Federal employees managed by Federal agencies. This privacy impact assessment is being conducted because the eOPF contains sensitive personally identifiable information about individuals.

Overview

Each Federal employee has a single personnel folder, known as the OPF (or Standard Form 66), which documents their entire period of Federal civilian service. The eOPF contains an electronic version (digital images) of the paper OPF for Federal employees, virtual work folders for use by human resource (HR) offices, and folders for non-federal employees that are accessible online. Employees with OPFs are those in the Executive Branch service, as listed in Title V of the United States Code, and some federal employees not under Title V.

The OPF contains records the Government needs to make accurate employment decisions throughout an individual's Federal career. Some of these records show that a federal appointment was valid (e.g., Appointment Affidavit and the Declaration for Federal Employment), or verify military service credit for leave, reduction-in-force, or retirement (e.g., DD 214, Certificate of Release or Discharge from Active Duty, and Military Service Deposit Election). The records also establish an individual's employment history, grades, occupations, and pay (e.g., Standard Form 50 and Notification of Personnel Action), and document choices made by the Federal employee under Federal benefits programs (e.g., Health Benefits Registration Form and the Designation of Beneficiary under the Federal Employees' Group Life Insurance Program).

**Privacy Impact Assessment**

Electronic Official Personnel Folder System (eOPF)

Page 2

Many federal agencies create their own virtual work folders in the eOPF. These folders store additional information on their federal employees, such as employee performance, payroll, staffing, security, benefit information.

The e-GOV initiative of the President's Management Agenda initiated in July 2001 challenged the Federal government to automate where it makes sense. The Office of Management and Budget (OMB) was charged with the implementation to reduce the amount of paper used by automating business processes. The Office of Personnel Management (OPM), working with the OMB, advised agencies that they had to convert the OPFs of their employees to an electronic format. The eOPF is the solution that OPM chose for the Federal government.

The eOPF combines document management with workflow capabilities, provides immediate access to personnel forms and information for a geographically dispersed workforce, and sends email notifications to employees when documents are added to their electronic folders. Added benefits of the system are the reduced costs associated with storage, maintenance, and retrieval of records, as well as integration with the agency's human resources information systems. The system also allows for compliance with OPM and federally mandated HR employee record management regulations.

The eOPF is available to authorized users via the Internet using Login.Gov, a Personal Identity Verification (PIV) card, or Entra ID credentials. Users are defined by their roles, which includes employee, agency HR Specialist, investigator, and agency administrator. For example, an employee can access the eOPF and view the equivalent of their own OPF, but they cannot modify their files or view another employee's OPF. An HR Specialist may only access the OPF and virtual work folders of employees to whom they provide HR services. Government officials who need to see the records in the eOPF to do their jobs are also given access. For example, investigators are granted access to the employee folders they are assigned to investigate. The



eOPF includes an audit trail that records when and why an individual reviewed a folder within the eOPF.

The eOPF system owner is the eOPF Program Management Office (eOPF PMO) and the eOPF business owner is also located in HRS. The eOPF is funded through interagency agreements with the eOPF participating agencies on a fiscal year basis and is administered through the OPM revolving fund.

The eOPF is currently available at <https://opf.opm.gov>.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

5 CFR 293.302, Establishment of Official Personnel Folder, requires an OPF to house records used by Federal government HR offices. These records document an employment history that includes grades, occupations and pay, and the employee's choices under Federal benefits programs. The records were maintained as paper in agency HR offices until they were converted to digital images as part of an e-Government initiative established in response to the E-Government Act of 2002.

In general, OPM collects, maintains, and uses the information in the eOPF pursuant to 5 U.S.C. 1104, 1302, 2951, 3301, and 4315; 3 CFR 1943-1948 Comp; 3 CFR 1954-1958 Comp; 5 CFR Part 293; 5 CFR 7.2; and Executive Orders 9830 and 12107.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The *OPM/GOVT 1, General Personnel Records*; *OPM/GOVT 2, Employee Performance File System Records*; and *OPM/GOVT 3, Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers* SORNs apply to the information maintained in the eOPF about Federal employees. Individual agencies who have records in



Privacy Impact Assessment
Electronic Official Personnel Folder System (eOPF)
Page 4

the eOPF that do not fall within the purview of the previously listed Government- wide SORNs have their own applicable SORNs.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes. The system security plan is part the Authority to Operate (ATO) package. The ATO for on-premises the eOPF system was granted (updated) on October 6, 2023.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, GRS 2.2, Item 040 (DAA-GRS-2017-0007-0004) covers the eOPF records and requires that they be destroyed when survivor or retirement claims are adjudicated or when records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use. This schedule does not necessarily apply to records that individual agencies choose to store in an agency-created virtual work folder or about non-Federal employees; those retention schedules would be set by the agency storing the records in the eOPF.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The PRA does not apply directly to the eOPF. While the eOPF is the ultimate repository for numerous forms, the program does not manage or regulate the collection of the information on the forms. The complete listing of forms in the eOPF can be found on the Master forms list at <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human-resources-integration/MasterFormsList/Index.aspx/>



Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The system collects, uses, disseminates, and maintains information about individuals and their federal employment. This information typically includes an employee's full name, date of birth (DOB), Social Security number (SSN), mailing address, home address, email address, telephone numbers, military service information, health and/or life insurance policy numbers, SSN of family members, DOB of family members, address of family members, bank account number, certificate/license numbers, civil or criminal history information, education records, and other identifying information.

In addition, the eOPF may contain information about past and present positions held; grades; salaries; duty station locations; notices of all personnel actions, such as appointments, transfers, reassignments, details, promotions, demotions, reductions-in-force, resignations, separations, suspensions, OPM approval of disability retirement applications, retirement, and removals; work experience; education level; specialized education or training obtained outside of Federal service; agency specific forms; and other documents relating to the recruitment, service history, payroll, benefits, retirement, performance and security clearance of an employee. For members of the Senior Executive Service, the eOPF may include information relating to sabbatical leave programs, reassignments, and details.

2.2. What are the sources of the information and how is the information collected for the project?

Individuals provide much of the information that goes into the eOPF through various personnel forms. The most common forms are the Oath of Office, health benefits registration and changes, life insurance registration and changes, resume, position description, employment eligibility verification, security clearance approval, designation of beneficiaries, Thrift Savings Plan



election and changes, veteran's preference designation and verification, and personnel actions. Additional information in the eOPF may be provided by the individual's supervisor or an HR specialist at their agency. Regardless of the source, the information is entered into another system used by the agency and then transferred to the eOPF as either a PDF or as data that the eOPF turns into a PDF using a predefined template.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the eOPF does not use information from commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

It is the responsibility of the individual employee providing information on personnel forms, and the agency or data provider collecting the data, to ensure its accuracy before submitting it to the eOPF. The eOPF does not validate the data submitted by the agencies and providers. Once a file is sent to the eOPF, federal employees and their HR specialists can access the eOPF to see the file, and federal employees should periodically review their information for accuracy and completeness.

Agencies are responsible for correcting errors in the data by following specific policy and guidance described in the Guide to Processing Personnel Actions (GPPA) and the Guide to Personnel Recordkeeping (GPR).

- The GPPA contains OPM's instructions on how to prepare personnel actions. It is available for viewing/printing on the OPM website: <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/#url%3DProcessing-Personnel-Actions>.
- The GPR describes general policies governing the creation, maintenance, and disposition of records used to document HR management programs established by OPM. It is available for



viewing/print on the OPM website: <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/personnel-recordkeeping/recguide2011.pdf>

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in the eOPF is not accurate or is filed incorrectly and, as such, will result in incorrect personnel decisions or benefit calculations.

Mitigation: This risk is mitigated by the fact that federal employees have full access to their information in the eOPF online to review their information and should periodically do that. In the event employees find errors in their eOPF information, or documents linked to them in the eOPF that do not belong to them, OPM has issued FAQs and other instructions so corrective measures can be taken. Agencies who submit information to the eOPF are also required to confirm it is accurate, complete, and filed correctly, based on the GPPA and GPR guidance.

Privacy Risk: There is a risk that the information collected in the eOPF is not about Federal employees and will not be used, retained, and disseminated properly.

Mitigation: OPM is mitigating this risk by working with each agency that maintains non-Federal employee data in the eOPF to determine whether the agency has appropriate measures in place concerning use, retention, and dissemination of that information.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

the eOPF aggregates and maintains records on current, separated, and retired Federal employees and non-Federal employees managed by Federal



agencies. The information is viewable through a secure user interface. Information is indexed/filed using the SSN in combination with the employee's full name and date of birth to validate the employee's identity and assure the correct filing of information.

The eOPF uses the information to enhance the HR workflow capabilities. the eOPF allows each employee to have a dedicated electronic personnel folder instead of a paper folder. This provides current federal employees immediate access to their personnel forms and information and notifies them when information in their eOPF is changed which requires the issuance of a corrected form.

The information in the eOPF is used by Federal agencies to make employment decisions throughout an employee's career. This includes personnel-related determinations, such as demonstrating that the appointment to federal services was valid; to verify military service credit for leave, reduction-in-force, or retirement; to establish an employment history, including grades, occupations and pay; and to document the choices an employee has made with respect to Federal benefits programs, including designating beneficiaries and selecting a health insurance carrier.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

Beginning in 2025, OPM plans to utilize artificial intelligence (AI) to extract various types of data from forms in the OPFs to analyze and verify the accuracy of the data with the goal of updating inaccurate information. Any use of AI will be done within a controlled environment, utilizing systems that have attained FedRAMP High authorization, and performed by approved OPM officials or qualified federal government contractors. The AI will employ stateless models, ensuring that inputs and outputs are not used to train, retrain, or improve base models. Before any AI is deployed in the system, comprehensive audit checks will be conducted to verify the accuracy of any



work performed. In addition, federal employees will be promptly notified by email of any changes to their records in the OPF that result in the issuance of a corrected form. Individual employees will have an opportunity to access and review any information in their eOPF records pursuant to sections 7.2 and 7.3 below.

The eOPF implements security and audit mechanisms that allow OPM IT staff to query the database and audit logs to detect trends/outliers associated with bad actor activity. OPM IT staff may also query the database to search for anomalies to assist with troubleshooting and resolving production issues.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

There are other OPM offices and programs with assigned roles and responsibilities within the eOPF. For example, OPM HR Specialists have read-write access to employees' eOPF records within their service area and OPM investigators have access to relevant records to conduct a suitability investigation. The eOPF employs role-based access controls, which categorize users and permit access according to their role. The other OPM offices with authority to access OPFs include:

- ***Retirement Services (RS):*** OPM Retirement Adjudicators processing retirement cases access the folders of retiring employees to verify their service and benefits eligibility.
- ***Merit System Audit & Compliance (MSAC):*** MSAC conducts HR evaluations examining a broad range of HR programs, including staffing and competitive hiring, performance management, and leadership and succession planning. MSAC evaluators access a sample of OPFs to review information such as employment history, educational degrees, and military service to accomplish those evaluations. The evaluators send advance information requests to the agency HR point of contact to specify the selected employees' OPFs included in the sample.



Privacy Impact Assessment
Electronic Official Personnel Folder System (eOPF)
Page 10

- **OPM and Agency Support:** OPM Support consists of HRS IT PMO Systems Capacity Branch, HRS IT PMO Recruitment Systems Branch, HRS IT PMO Software Quality Assurance Branch, Chief Information Security Officer, OPM Enterprise Information Services, and OPM Office of Inspector General personnel.
- **OPM Data Management:** HRS may access an eOPF record when a request to access or amend that record is requested pursuant to the Privacy Act.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that unauthorized users may access the information in the eOPF and use it for purposes that are inconsistent with the personnel purposes for which it was collected.

Mitigation: This risk is mitigated by using role-based access controls, which only permit designated individuals to access information they need to know to perform their job responsibilities.

Privacy Risk: There is a risk that authorized users may access information that they are not authorized to see or use information for an unauthorized purpose such as performing searches on themselves, friends, relatives, or neighbors. Also, authorized users may inappropriately disclose this information, either intentionally or unintentionally.

Mitigation: This risk is mitigated by using role-based access controls, which limit the information authorized users can access to that which they need to know. In addition, OPM conducts periodic security audits, regularly monitors security practices, and requires users to agree to rules of behavior to indicate they understand and will adhere to appropriate data use.



Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals who access the eOPF to view their own personnel records may review the eOPF Privacy Policy, which addresses the collection and use of information. In addition, individuals are provided with notice through the Privacy Act statements on the various forms that ultimately become a part of their eOPF records. Notice concerning the collection and use of the information in the eOPF is also provided via the SORNs listed in question 1.2 and through this PIA

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may decline to provide information on the various personnel forms that are entered into the eOPF, although there may be consequences to not providing information, as explained in the Privacy Act statements on those forms. Once individuals provide information on those forms, the Federal agencies using the eOPF determine what information is sent to the eOPF; there is no ability to consent to particular uses of information in the eOPF or for individuals to decline to have their information included in the system.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that their information will be placed in the eOPF and accessed and used for various personnel reasons.

Mitigation: This risk is mitigated by placing Privacy Act statements on various agency forms that inform individuals why and for what purpose their information is being collected. In addition, individuals are provided notice concerning the eOPF through the Privacy Policy they are provided when



accessing their records and via the SORNs referenced in Section 1.2 and this PIA.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

When an employee leaves an agency, the OPF is transferred to either the National Personnel Records Center (NPRC) or the employee's new agency. The losing agency purges the OPF and work folders in the eOPF and, at that point, the employee and the losing agency personnel no longer have access to the records. If the employee is going to a new agency, the new agency grants access to the employee and appropriate HR specialists, Investigators, and system administrators.

The electronic versions of the OPFs for Federal employees who do not continue in another agency are maintained in the eOPF in an area managed by NPRC. NPRC is one of the National Archives and Records Administration's (NARA) largest operations and is the central repository of personnel-related records for both the military and civil services of the United States Government. Past employees cannot directly access their records in the eOPF once stored by NPRC; they need to request that information from NPRC.

The records are retained pursuant to the records schedule identified in Section 1.4.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in the eOPF will be retained longer than is necessary for its intended business purpose.

Mitigation: This risk is mitigated by requiring adherence to the appropriate records retention schedule and by providing guidance to the eOPF users in the GPR, which describes general policies governing the creation,



maintenance, and disposition of records used to document HR management programs established by OPM. OPM cannot enforce the adherence to policy, or the retention schedule practices at other agencies. However, NARA guidance does dictate compliance.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As part of the normal agency operations, eOPF data is generally not shared beyond the agency where an employee works. The information in the eOPF is used by Federal agency HR offices to make employment decisions throughout an employee's career. In addition, the information in the eOPF may be shared for background investigation purposes with Defense Counterintelligence and Security Agency (DCSA) investigators, who need access to complete investigations such as initial background checks and the renewal of existing investigations. DCSA is not authorized to conduct a background investigation unless a release, signed by the subject of the investigation, is received. eOPF data may also be shared with HRS's Enterprise Human Resource Integration (EHRI) system to facilitate data analytics for OPM program offices and agency HR partners.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing described above is consistent with the purposes for which the information was collected, as documented in the applicable SORNS listed in Section 1.2. In general, this includes for personnel-related determinations, such as demonstrating that the appointment to Federal services was valid; to verify military service credit for leave, reduction-in-force, or retirement; to establish an employment history, including grades, occupations and pay; and the choices an employee has made with respect to Federal benefits programs, including designating beneficiaries and



selecting a health insurance carrier.

6.3. Does the project place limitations on re-dissemination?

OPM does not explicitly limit the re-dissemination of eOPF information by the agencies. However, those agencies are required to adhere to the government wide SORNs referenced in Section 1.2, or their own SORNs if information is not covered under the government-wide SORNs. This means they cannot re-disseminate the information except pursuant to an applicable routine use or as otherwise permitted by the Privacy Act.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The eOPF contains automated audit log capabilities that record all access and review of the information in the system, as well as the reason for the review. The eOPF also have manual processes that require documentation, justification and approval of all access, reviews, and removal of data that occurs outside the automated audit log functionality.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information will be disclosed and used for a purpose that is not consistent with the purposes for which it was originally collected.

Mitigation: This risk is mitigated by limiting access to the eOPF to individuals with a need to know to perform their official duties, by careful review of any routine use disclosure decisions, by requiring contractors and consultants accessing the system to sign non-disclosure agreements, and by adding provisions in MOUs with participating agencies and programs that require the recipients of the information to use it only for the purpose for which it is provided. Each eOPF data set targeted for ingestion into the HRS HR platform for data analysis purposes will be assessed via a privacy impact assessment.



Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

Individual employees may access their own OPF via the authentication method issued by their agency (e.g., PIV). In addition, individuals can submit a Privacy Act request for their records by following the process outlined in the applicable SORNs listed in 1.2.

Individuals requesting access must comply with OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297). Current Federal employees should contact the Personnel Officer or other responsible official of their agency. Former Federal employees should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118.

In general, individuals must furnish the following information for their records to be located and identified:

- Full name(s).
- Date of birth.
- Social security number.
- Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).
- Signature.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals employed by a federal agency can contact their human resources office and ask to correct any inaccurate or erroneous information in their eOPF records.

Like requests for access, individuals can also submit a Privacy Act request to amend their records following the process outlined in the applicable SORNs listed in 1.2. Current Federal employees should contact the official



designated at their current agency. Former employees should contact the Office of Personnel Management using the process and contact information located on the applicable SORN. Individuals must furnish the following information for their records to be located and identified.

- Full name(s).
- Date of birth.
- Social security number.
- Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).
- Signature.

7.3. How does the project notify individuals about the procedures for correcting their information?

Email notifications are sent to employees when documents are added to their eOPF folders, including when corrections are made to the records in their eOPF that result in the issuance of an updated form. The notifications contain instructions indicating the employee should review the new document(s) and notify their HR office if there is inaccurate or erroneous information. In addition, the SORNs referenced in Section 1.2 provided instructions to individuals who wish to request an amendment to their records.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not understand how to access and correct their records in the eOPF.

Mitigation: This risk is mitigated through publishing clear instructions on various OPM and agency websites, in the SORNs, and in this PIA informing individuals how to access and request amendment to their records. Further assistance to gain access or make amendments is given in the eOPF within the online FAQs that can be viewed by clicking the word 'FAQ' at the top of the login page within the web site. The instructions in the FAQs can be printed.



Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

The eOPF contains automated audit log capabilities that record all access and review of the information contained in the system as well as the reason for the review. All activities performed in the eOPF are logged and the audit logs are periodically reviewed to ensure that the information is being accessed and used appropriately.

In addition, the eOPF includes security features to protect the integrity of user information including requiring agencies to limit access to the minimal level that allows normal functioning.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees and contractors who support the eOPF must complete OPM-provided, mandatory, annual Security and Privacy Awareness Training prior to gaining access to the eOPF. In addition, OPM offers training to HR Specialists and employees designated as systems administrators specific to the eOPF. This training stresses the importance of protecting personally identifiable information and teaches the individuals to navigate through the eOPF to complete their work assignments.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

The eOPF employs role-based access controls, which categorize users as employee, Investigator, HR Specialist, or agency administrator and permit access according to their role. The agencies that submit information to the eOPF determine which of their HR Specialists require access.



8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

When an agency elects to use the eOPF, the OPM security staff works with the agency to enter into an ISA and MOU. These are reviewed by relevant OPM stakeholders and signed by both parties. The ISAs and MOUs are updated every three years or when there are changes to the system.

Responsible Officials

Nii-Kwashie Aryeetey
Director, eOPF Program
Human Resources Solutions Information Technology Program Management
Office (HRSITPMO)

Approval Signature

Becky Ronayne
Acting Senior Agency Official for Privacy